REMARKS

Applicants thank the Examiner for total consideration given the present application. Claims 1-24 are currently pending of which claims 1, 9, and 17 are independent. Claims 1, 5, 9, 13, and 17 have been amended through this Reply. Applicants respectfully request reconsideration of the rejected claims in light of the amendment and remarks presented herein, and earnestly seek timely allowance of all pending claims.

SPECIFICATION

The Specification has been amended merely to address informal issues and to enhance clarity.

FORM 1449 ACKNOWLEDGMENT REQUESTED

It is noted that the Examiner has not considered the Uchiyama (CA) reference. The Examiner alleges that no legible copy was provided. A legible copy of the Uchiyama (CA) reference has been submitted herewith. Accordingly, Applicants respectfully request the Examiner to consider the Uchiyama (CA) reference and provide an initialed copy of the PTO-1449 for the present application.

35 U.S.C. § 103 REJECTION – Yamazaki, Bennett, Kou, Chung, Wu

A. Claims 1, 9 and 17 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Yamazaki (Institute of Electronics, Information and Communication Engineer's Society Conference 2001)[hereinafter "Yamazaki"] in view of Bennett et al. ("Quantum Cryptography: Public Key Distribution and Coin Tossing" 1984)[hereinafter "Bennett"]. Applicants respectfully traverse this rejection.

For a Section 103 rejection to be proper, a *prima facie* case of obviousness must be established. *See M.P.E.P. 2142.* One requirement to establish *prima facie* case of obviousness is that the prior art references, when combined, must teach or suggest all claim limitations. *See*

M.P.E.P. 2142; M.P.E.P. 706.02(j). Thus, if the cited references fail to teach or suggest one or more elements, then the rejection is improper and must be withdrawn.

In this instance, it is respectfully submitted that neither Yamazaki nor Bennett, alone or in combination, teach or suggest all claim limitations.

For example, independent claim 1 recites, *inter alia*, "a cryptographic key creation step of each of the first communication apparatus and the second communication apparatus ***discarding a part of pieces of the common information*** after correction ***according to public error correction information***, ***creating a cryptographic key*** using information that ***has remained after discarding including the amount of information of n-k bits***, and setting the cryptographic key as ***a common key*** which is ***shared*** between first communication apparatus and the second communication apparatus."

The Examiner acknowledges that Yamazaki fails to teach or suggest the above-identified claim feature. Thus, the Examiner imports Bennett in order to fulfill this deficiency of Yamazaki. It is respectfully submitted that Bennett also fails to teach or suggest the above-identified claim feature.

Bennett is directed to a conventional quantum public key distribution method in which, instead of using the quantum channel for directly sending a meaningful messages, the quantum channel is used for transmitting random bits between two users who share no secret information initially. (*See col. 4, section III.*) In this conventional quantum key distribution method, an error communication path is not considered. Thus, when an error is present, the common data (common key) is discarded because an intercepting action is presumed to be present. (*See col. 4, section III.*)

This conventional quantum key distribution method of Bennett inherently includes a problem that creation efficiency of the common key is correspondingly affected in some transmission paths. Further, the conventional method that can correct the data error on the transmission path, huge number of exchanges of the parity is generated for specifying the error bit, and the error correction processing is also performed in a predetermined time by the random permutation. Thus, there are additional problems associated with the conventional quantum

public key distribution method of Bennett that a long period of time is required for the error correction processing.

The claimed invention solves the above-noted problems associated with the conventional quantum public key distribution method by providing a cryptographic key creation step of each of a first communication apparatus (transmitter) and a second communication apparatus (receiver) ***discarding a part of pieces of a common information*** after correction ***according to public error correction information***, ***creating a cryptographic key*** using information that ***has remained after discarding including the amount of information of n-k bits***, and setting the cryptographic key as ***a common key*** which is ***shared*** between the transmitter and the receiver.

Thus, the claimed invention provides a quantum key distribution method that can create a highly-secured common key while correcting data error on a transmission path by an error correction code having remarkably high characteristics. According to the claimed invention, the ***data error of the common information is corrected*** by a deterministic and stable-characteristics parity check matrix for "Irregular-LPDC code", and a part of the common information is discarded depending on the ***public error correction information***.

The claimed invention is distinguished from the Bennett reference in that although Bennett may disclose a method of creating a cryptographic public-key, nowhere does Bennett teach or suggest a cryptographic key creation step which ***discards a part of pieces of a common information*** after correction ***according to public error correction information***, creates ***a cryptographic key*** using information that ***has remained after discarding including the amount of information of n-k bits***, and sets the cryptographic key as ***a common key*** which is ***shared*** between the transmitter and the receiver.

Conversely, in Bennett, if transmission has been disturbed, the two users (one in the transmission side and the other in the reception side) ***discard the shared secret bits*** and ***try again***, deferring any meaningful communication ***until they have succeeded in transmitting enough random bits*** through a quantum channel to serve as a ***one-time pad***. (*See col. 4, section III.*) For example, when even one piece of the confirmed data does not correspond to the data owned by the transmitter or the receiver, judging that the interceptor is present, the two users of

Bennett discard the common data and perform the process of sharing the key again from the start. On the other hand, when the confirmed data completely corresponds to the data owned by the transmitter of the receiver, judging that there is no interceptor, the transmitter and the receiver discard the data used for the confirmation, and the saved common data becomes the common key for the transmitter and the receiver.

Thus, at least for the above reasons, it is respectfully submitted that Bennett cannot teach or suggest a cryptographic key creation step which ***discards a part of pieces of a common information*** after correction ***according to public error correction information***, creates ***a cryptographic key*** using information that ***has remained after discarding including the amount of information of n-k bits***, and sets the cryptographic key as ***a common key*** which is ***shared*** between the transmitter and the receiver as recited in independent claim 1.

Independent claim 9 is directed to a communication apparatus on transmission side which includes, among other features, a cryptographic key creation unit that ***discards a part of pieces of the common information*** after error correction ***according to public error correction information***, ***creates a cryptographic key*** using information that ***has remained after discarding including the amount of information of n-k bits***, and sets the cryptographic key as ***a common key*** which is ***shared*** with the communication apparatus on the reception side.

Independent claim 17 is directed to a communication apparatus on reception side which includes, among other features, a cryptographic key creation unit that ***discards a part of pieces of the common information*** after error correction ***according to public error correction information***, ***creates a cryptographic key*** using information that ***has remained after discarding including the amount of information of n-k bits***, and sets the cryptographic key as ***a common key*** which is ***shared*** with the communication apparatus on the transmission side.

As demonstrated above in great detail with respect to claim 1, neither Yamazaki nor Bennett, alone or in combination, teaches or suggest the above-identified features of claims 9 and 17.

Therefore, for at least these reasons, it is respectfully submitted that claims 1, 9, and 17 are distinguishable from Yamazaki and Bennett. Accordingly, withdrawal of the obviousness rejection of claims 1, 9, and 17 based on Yamazaki and Bennett is earnestly solicited.

B. Claims 2, 7, 10, 15, 18, and 23 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Yamazaki in view of Bennett, and further in view of Kou et al. (IEEE Globecom([hereinafter "Kou] and Chung et al. (IEEE Transactions on Information Theory([hereinafter "Chung"]. Claims 8, 16 and 24 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Yamazaki in view of Bennett, Chung and Kou, and further in view of Wu et al. ("Generalized inverses in public key cryptosystem design" 1998)[hereinafter "Wu"]. Claims 3-6, 11-14, and 19-22 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Yamazaki in view of Bennett, and further in view of Wu. These rejections are respectfully traversed.

As demonstrated above, the combination of Yamazaki and Bennett fails to teach or suggest all limitation of independent claims 1, 9, and 17. Claims 2-8, 10-16, and 18-24 are at least distinguishable from Yamazaki and Bennett by virtue of their dependency on corresponding independent claims 1, 9, and 17. Kou, Chung, and Wu have not been, and indeed cannot be, relied upon to fulfill the deficiency of Yamazaki and Bennett.

Therefore, for at least theses reasons, it is respectfully requested to withdraw the rejection of claims 2-8, 10-16, and 18-24.

CONCLUSION

In view of the above amendment, Applicants believe the pending application is in condition for allowance.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Ali M. Imam Reg. No. 58,755 at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.17; particularly, extension of time fees.

Dated: March 4, 2009

Respectfully submitted,

By _____ #58,755
Michael K. Mutter
Registration No.: 29,680
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicants